



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Determination of the Order of the Groups of Isomorphisms of the Groups of Order p^4 , where p is a Prime.

BY ROSS W. MARRIOTT.

It is well known that the group of isomorphisms of a group G , of prime order p , is a group of order $p-1$, and that the group of isomorphisms of a group of order p^2 is a group of order $p(p-1)$ and cyclic, if the group of order p^2 be cyclic. It is isomorphic with the linear homogeneous group on p^2 variables (mod p), if the group of order p^2 be not cyclic.

Western in his paper, "Groups of Order p^3q ," *Proceedings of London Mathematical Society*, Vol. XXX, treated the isomorphisms of groups of order p^3 .

A knowledge of the groups of isomorphisms of a group is essential in the work of constructing groups having the given group as a subgroup. The isomorphisms of the groups of order p , p^2 , p^3 are of fundamental importance for example in the work of tabulating all groups of the orders p^{2*} , $p^2q\dagger$, $p^2qr\dagger$, $p^3§$, $p^3q||$.

It is obvious that the determination of the orders of the groups of isomorphisms of all groups of order p^4 must precede the tabulation, for example, of all types of groups of order p^4q . This latter tabulation is logically the next problem of this character which remains to be undertaken, the orders $p^5||$, p^3q^{2**} , $pqrst\dagger\dagger$ having been previously treated.

It is the purpose of this paper to determine the order of the groups of isomorphisms of all groups of order p^4 . For the sake of convenient references,

* Burnside, "Theory of Groups"; Young, "On the Determination of Groups whose Order is the Power of a Prime, *AMERICAN JOURNAL OF MATHEMATICS*, Vol. XV (1893); Cole and Glover, *AMERICAN JOURNAL OF MATHEMATICS*, Vol. XV (1893).

† Burnside, "Theory of Groups"; Cole and Glover, *AMERICAN JOURNAL OF MATHEMATICS*, Vol. XV (1893).

‡ O. E. Glenn, *Trans. of Amer. Math. Soc.*, Vol. VII, No. 7.

§ Burnside, "Theory of Groups"; Young, *loc. cit.*; Cole and Glover, *loc. cit.*

|| Western, *Proc. of London Math. Soc.*, Vol. XXX.

¶ Bagnara, *Armati di Matematica* (1898), pp. 137-228.

** M. O. Tripp, "Groups of Order p^3q^2 ."

†† Hölder, *Göttinger Nachrichten* (1895), pp. 211-229.

I shall recall a few of the well-known definitions and theorems, regarding isomorphisms.

Suppose two groups, G and G' , are so related that to each element, g' of G' , corresponds one or more elements, $g, g_1, g_2, \dots$ of G ; while reciprocally to each element, g of G , corresponds one or more elements, $g', g'_1, g'_2, \dots$ of G' . Suppose further, that if g_i and g_j are elements of G corresponding to elements g'_i and g'_j of G' , $g_i g_j$ is an element of G corresponding to $g'_i g'_j$ of G' . Then, G and G' are said to be isomorphic.

If l elements of G correspond to each element of G' , and k elements of G' correspond to each element of G , G and G' are said to have an (l, k) isomorphism with each other. The most important case is that in which $l=k=1$. Then G and G' are called simply isomorphic. Or, what is the same thing, if G and G_0 be two groups of equal order, and if a correspondence can be established between the operations of G and G_0 , so that to every operation of G there corresponds a single operation of G_0 , and to every operation of G_0 there corresponds a single operation of G , while to the product PQ of any two operations of G , there corresponds the product $P_0 Q_0$ of the corresponding operations of G_0 , the groups G and G' are said to be simply isomorphic.

Again, if the correspondence between the operations of a group G be such that to every operation P there corresponds a single operation P_0 , while to the product PQ of two operations there corresponds the product $P_0 Q_0$ of the corresponding operations, it is said to define an isomorphism of the group G with itself.

The elements $P, Q, R, S, T, \dots$ of a group are called independent if no one of them can be expressed as a product of powers of the others,—thus P is not expressible in the form $Q^a R^b S^c \dots$.

A group is said to be determined abstractly when we know the number of elements it contains, and the way in which any two combine by multiplication. Hence, the group is given abstractly by a set of generating elements, and certain independent and mutually consistent relations which they satisfy. Two groups, G and G_0 , having the same number of elements, combining according to the same laws abstractly considered, are one and the same group.

THEOREM. *The order of the group of isomorphisms of a group G is equal to the number of ways that the group G can be made simply isomorphic with itself, and this is equal to the number of ways the generators can be chosen from the elements of G so that they will obey those laws, and only those laws which define the group abstractly.*

Let us suppose $P, Q, R, S, \dots$ are generators of a group G , satisfying certain relations, and $P_0, Q_0, R_0, S_0, \dots$ are elements of G satisfying pre-

eisely similar relations but no relations independent of these. Let these define the group G_0 . Then an isomorphism ($G_0 \sim G$) of G exists in which P corresponds to P_0 , Q to Q_0 , R to R_0 , etc.

For G and G_0 having the proper correspondence between their elements are simply isomorphic, but as the elements of G_0 are also elements of G , this simply isomorphic property exhibits an isomorphism ($G_0 \sim G$) of G with itself. Hence an isomorphism of G exists, where P corresponds to P_0 , Q to Q_0 , etc.

Now to each way of choosing the elements $P_0, Q_0, R_0, \dots$ of G_0 , corresponds a distinct isomorphism of G . The symbol of an isomorphism defines an operation simply isomorphic with a substitution performed upon the elements of the group G , the totality of these operations forms a group* simply isomorphic with the group of isomorphisms of the group G . Hence, the order of the group of isomorphisms is the number of ways of selecting the generators P_0, Q_0, R_0 , etc.

Our general method of procedure in the present problem is to take for the generating elements the most general operations in the group G , of order p^4 ; i. e., to assume the new generators in the form:

$$\begin{aligned} P_0 &= P^x Q^y R^z S^w \dots, \\ Q_0 &= P_1^x Q_1^y R_1^z S_1^w \dots, \\ R_0 &= P_2^x Q_2^y R_2^z S_2^w \dots, \\ S_0 &= P_3^x Q_3^y R_3^z S_3^w \dots, \\ &\dots\dots\dots \end{aligned}$$

where $P, Q, R, \dots$ are the generators of G , to impose on the exponents the conditions necessary to make the new generators obey the defining relations of G , to subject the exponents to the conditions such that the new generators have no other relations existing among them. These conditions will be sufficient to insure that the new generators are independent, and so may be taken to generate the group.

This method leads always to a set of congruences, the number of solutions of which, is the number of ways the new generators may be chosen and therefore gives the order of the group of isomorphisms of the group under consideration.

The groups are considered in the order in which they are tabulated in Burnside, "Theory of Groups," pp. 87, 88, 89. Nine of the first ten groups require no separate investigation when p is an even prime. Number 7, how-

* Burnside, "Theory of Groups," 156.

ever, requires an independent procedure when p is 2. The types of G_{p^4} which exist only when p is even are treated in the latter part of the paper.

The transformation formulæ have been developed by mathematical induction, and are given for each non-abelian group.

Certain applications to the theory of numbers in connection with the determinants which enter into the congruences for certain of the types is another interesting feature of the details of the paper.

With the exception of three types, every group of order p^4 has a group of isomorphisms of an order of the general form $N=p^a(p-1)^b(p+1)^c$. Two of the exceptions are of the form $N=2p^a(p-1)^b(p+1)^c$.

The notation in the paper is practically the same as in Burnside, "Theory of Groups."

Section 1.

$$P^4=1.$$

Let $P_0=P^x$ be a new generator. It will generate the group provided x is prime to p . The group contains $p^3(p-1)$ operations of order p^4 . Hence,

$$N=p^3(p-1).^*$$

Section 2.

$$P^{p^3}=1, Q^p=1, Q^{-1}PQ=P.$$

Let $P_0=P^xQ^y$, $Q_0=P^{x_1}Q^{y_1}$. Then,

$$P_0^{p^3}=1, \therefore x \not\equiv 0 \pmod{p}, \dagger \quad (1)$$

$$Q_0^p=1, \therefore x_1 \equiv 0 \pmod{p^2}. \quad (2)$$

The conditions (1) and (2) are sufficient to insure the independence of the generators so far as their powers prime to p are concerned.

Suppose $P_0^h Q_0^k = 1$, where $k \not\equiv 0 \pmod{p}$,

$$\therefore \begin{cases} hx + kx_1 \equiv 0 \pmod{p^3}, \\ hy + ky_1 \equiv 0 \pmod{p}. \end{cases}$$

Since $x \not\equiv 0 \pmod{p}$ and $x_1 \equiv 0 \pmod{p^2}$, we must have $h \equiv 0 \pmod{p^2}$, and hence, also, $y_1 \equiv 0$.

Now, if $y_1 \not\equiv 0 \pmod{p}$, the generators P_0 and Q_0 are independent,

$$\therefore y_1 \not\equiv 0 \pmod{p}. \quad (3)$$

There being no restrictions on y , there are $p^4(p-1)^2$ ways of choosing the generators,

$$\therefore N = p^4(p-1)^2.$$

* Throughout the paper N denotes the order of the group of isomorphisms.

† And no less power of P_0 is unity. This will be understood hereafter.

Section 3.

$$P^{p^2}=1, Q^{p^2}=1, Q^{-1}PQ=P.$$

Let $P_0=P^xQ^y$, $Q_0=P^{x_1}Q^{y_1}$. Then,

x and y cannot be simultaneously $\equiv 0 \pmod{p}$,
 x_1 and y_1 cannot be simultaneously $\equiv 0 \pmod{p}$.

Suppose $P_0^h Q_0^k=1$, h and k prime to p . This gives:

$$\begin{aligned} & \left. \begin{aligned} hx+kx_1 &\equiv 0 \\ hy+ky_1 &\equiv 0 \end{aligned} \right\} \pmod{p^2}, \\ \therefore \begin{vmatrix} x & x_1 \\ y & y_1 \end{vmatrix} &\not\equiv 0 \pmod{p^2}. \end{aligned} \quad (1)$$

Condition (1) insures the independence of P_0 and Q_0 so far as their powers prime to p are concerned. Suppose now

$P_0^{h'p} Q_0^{k'p}=1$, h' and k' prime to p . This gives:

$$\begin{aligned} & \left. \begin{aligned} h'px+k'px_1 &\equiv 0 \\ h'py+k'py_1 &\equiv 0 \end{aligned} \right\} \pmod{p^2}, \\ \therefore \begin{vmatrix} x & x_1 \\ y & y_1 \end{vmatrix} &\not\equiv 0 \pmod{p}. \end{aligned} \quad (2)$$

Conditions (1) and (2) are sufficient to insure that P_0 and Q_0 generate the group. The number of solutions which satisfy (1) is

$$p^3(p^2-1)(p-1)(p^2+p-1),$$

and this is the number of ways a pair of generators of order p^2 may be chosen. Of these solutions, the number which fail to satisfy condition (2) is

$$p^3(p-1)^3(p+1).$$

The number of ways of choosing the generators is

$$N=p^3(p^2-1)(p-1)(p^2+p-1)-p^3(p-1)^3(p+1)=p^5(p-1)^2(p+1).$$

Section 4.

$$P^{p^2}=1, Q^p=1, R^p=1, Q^{-1}PQ=P, R^{-1}PR=P, R^{-1}QR=Q.$$

Let P_0, Q_0, R_0 be defined as above,

$$P_0^{p^2}=1, \therefore x \not\equiv 0 \pmod{p}, \quad (1)$$

$$Q_0^p=1, \therefore x_1 \equiv 0 \pmod{p}, \quad (2)$$

$$R_0^p=1, \therefore x_2 \equiv 0 \pmod{p}. \quad (3)$$

Let $x_1 = x'p$ and $x_2 = x''p$. Then,

$$\left. \begin{array}{l} x', y_1 \text{ and } z_1 \text{ are not simultaneously } \equiv 0 \\ x'', y_2 \text{ and } z_2 \text{ are not simultaneously } \equiv 0 \end{array} \right\} \pmod{p}.$$

For, if they were, Q_0 and R_0 would be unity.

Suppose $P_0^h Q_0^k R_0^m = 1$, k and m prime to p ,

$$\therefore \left\{ \begin{array}{l} hx + kpx' + mpx'' \equiv 0 \pmod{p^2}, \\ hy + ky_1 + my_2 \equiv 0 \\ hz + kz_1 + mz_2 \equiv 0 \end{array} \right\} \pmod{p}.$$

That this may be satisfied requires $h \equiv 0$, and also $\begin{vmatrix} y_1 & y_2 \\ z_1 & z_2 \end{vmatrix} \equiv 0 \pmod{p}$.

Hence, we must have

$$\begin{vmatrix} y_1 & y_2 \\ z_1 & z_2 \end{vmatrix} \not\equiv 0 \pmod{p}. \quad (4)$$

The conditions (1), (2), (3), (4) are sufficient to insure the generators P_0 , Q_0 and R_0 independent.

There are $p(p-1)^2(p+1)$ solutions of (4); x has $p(p-1)$ values, x' , x'' , y and z , each has p values,

$$\therefore N = p^6(p-1)^3(p+1).$$

Section 5.

$$P^p = Q^p = R^p = S^p = 1, PQ = QP, RP = PR, PS = SP, QR = RQ, QS = SQ, RS = SR.$$

As before, P_0 , Q_0 , R_0 , S_0 are new generators. Since every operation of the group is of order p , these new generators satisfy the defining relations without condition. Suppose there is a relation $P_0^h Q_0^k R_0^l S_0^m = 1$. We get

$$\left\{ \begin{array}{l} hx + kx_1 + lx_2 + mx_3 \equiv 0 \\ hy + ky_1 + ly_2 + my_3 \equiv 0 \\ hz + kz_1 + lz_2 + mz_3 \equiv 0 \\ hw + kw_1 + lw_2 + mw_3 \equiv 0 \end{array} \right\} \pmod{p}.$$

If these congruences do not co-exist, the new operations are independent, and will generate the group. The condition is fulfilled if

$$\begin{vmatrix} x & x_1 & x_2 & x_3 \\ y & y_1 & y_2 & y_3 \\ z & z_1 & z_2 & z_3 \\ w & w_1 & w_2 & w_3 \end{vmatrix} \not\equiv 0. \quad (1)$$

The number of sets of values which satisfy (1) is

$$N = (p^4 - 1)(p^4 - p)(p^4 - p^2)(p^4 - p^3).$$

Section 6.

$$P^{p^3}=1, Q^p=1, Q^{-1}PQ=P^{1+p^2}.$$

The transformation formulæ for this group are:

$$P^x Q^y = Q^y P^{x(1+p^2)y}, \quad (1)$$

$$Q^y P^x = P^{x(1-p^2y)} Q^y, \quad (2)$$

$$[P^x Q^y]^k = P^{kx - \frac{1}{2}k(k-1)xy p^2} Q^{ky}, \quad (3)$$

$$P_0^{p^3}=1, \therefore x \not\equiv 0 \pmod{p}, \quad (4)$$

$$Q_0^p=1, \therefore x_1 \equiv 0 \pmod{p^2}. \quad (5)$$

Let $x_1 = x' p^2$.

$$Q_0^{-1} P_0 Q_0 = P_0^{1+p^2}, \therefore y_1 \equiv 1 \pmod{p}, \text{ i. e., } y_1 = 1. \quad (6)$$

Suppose now $P_0^k Q_0^k = 1$.

The application of transformation equation (3) leads to a set of congruences inconsistent with those obtained from the defining relations. Hence,

$$N = p^4(p-1), \text{ whether } p \text{ is odd or even.}$$

Section 7.

$$P^{p^2}=1, Q^p=1, R^p=1, R^{-1}QR=QP^p, QP=PQ, RP=PR.$$

The transformation formulæ for this group are:

$$Q^y R^z = R^z Q^y P^{yzp}, \quad (1)$$

$$P^x Q^y R^z = P^{x+yzp} R^z Q^y, \quad (2)$$

$$[P^x Q^y R^z]^k = P^{kx - \frac{1}{2}k(k-1)yzp} Q^{ky} R^{kz}. \quad (3)$$

Let P_0, Q_0 and R_0 be new generators.

$$P_0^{p^2}=1, \therefore x \not\equiv 0 \pmod{p}, \quad (4)$$

$$Q_0^p=1, \therefore x_1 \equiv 0 \pmod{p}, \quad (5)$$

$$R_0^p=1, \therefore x_2 \equiv 0 \pmod{p}, \quad (6)$$

$$R_0^{-1} P_0 R_0 = P_0, \therefore \begin{vmatrix} y & y_2 \\ z & z_2 \end{vmatrix} \equiv 0 \pmod{p}, \quad (7)$$

$$Q_0^{-1} P_0 Q_0 = P_0, \therefore \begin{vmatrix} y & y_1 \\ z & z_1 \end{vmatrix} \equiv 0 \pmod{p}, \quad (8)$$

$$R_0^{-1} Q_0 R_0 = Q_0 P_0^p, \therefore \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix} \equiv x \pmod{p}. \quad (9)$$

Let now $P_0^h Q_0^k R_0^l = 1$, and apply the transformation formulæ (1), (2), (3). There results a congruence contrary to (9). Thus the defining relations of the group determine the conditions which insure that P_0, Q_0 and R_0 are independent. We have now to find the number of solutions of the congruences (4)–(9) in-

clusive. (4) and (9) are the sufficient conditions that (7) and (8) have only zero solutions. Hence, the number of solutions is, when p is odd,

$$N = p^4(p-1)^2(p+1).$$

Suppose now that $p=2$. In this case we have the congruences

$$x \not\equiv 0, x_1 - y_1 z_1 \equiv 0, x_2 - y_2 z_2 \equiv 0, x \equiv z_2 y_1 - y_2 z_1, y \equiv z \equiv 0, \text{ all (mod } 2),$$

$$\therefore N = 3 \cdot 2^3.$$

Section 8.

$$P^{p^2}=1, Q^{p^2}=1, Q^{-1}PQ=P^{1+p}.$$

The transformation formulæ for this group are:

$$P^x Q^y = Q^y P^{x(1+p)^y}, \quad (1)$$

$$Q^y P^x = P^{x(1+p)^{-y}} Q^y, \quad (2)$$

$$[P^x Q^y]^k = P^{kx - \frac{1}{2}k(k-1)xy} Q^{ky}. \quad (3)$$

Neither x and y nor x_1 and y_1 can be simultaneously $\equiv 0 \pmod{p}$. Else P_0 and Q_0 are not of order p^2 .

$P_0^{p^2}=1$ and $Q_0^{p^2}=1$, without any condition on the exponents.

$$Q_0^{-1}P_0Q_0=P_0^{1+p}, \therefore y \equiv 0, x \equiv xy_1 - yx_1 \pmod{p}. \quad (4)$$

Let $P_0^h Q_0^k = 1$. This leads to a set of conditions inconsistent with the conditions obtained from the defining relations,

$$\therefore N = p^5(p-1).$$

Section 9.

$$P^{p^2}=Q^p=R^p=1, PR=RP^{1+p}, PQ=QP, RQ=QR.$$

The transformation formulæ are, for this group:

$$P^x R^z = R^z P^{x(1+p)^z}, \quad (1)$$

$$R^z P^x = P^{x-xzp} R^z, \quad (2)$$

$$P^x Q^y R^z = R^z P^{x(1+p)^z} Q^y, \quad (3)$$

$$[P^x Q^y R^z]^k = R^{kz} P^{kx} [1 + \frac{p^z(k+1)}{2}] Q^{ky}. \quad (4)$$

$$P_0^{p^2}=1. \text{ Hence, } x \not\equiv 0 \pmod{p}, \quad (5)$$

$$Q_0^p=1. \quad x_1 \equiv 0 \pmod{p}, \quad (6)$$

$$R_0^p=1. \quad x_2 \equiv 0 \pmod{p}, \quad (7)$$

$$R_0^{-1}P_0R_0=P_0^{1+p}. \quad z_2 \equiv 1 \pmod{p}, \quad (8)$$

$$P_0^{-1}Q_0P_0=Q_0. \quad z_1 \equiv 0 \pmod{p}, \quad (9)$$

$$R_0^{-1}Q_0R_0=Q_0. \text{ This requires no further conditions.}$$

Let $P_0^h Q_0^k R_0^m = 1$.

The transformation formulæ show that we must impose the further condition $y_1 \not\equiv 0$, if the generators P_0, Q_0, R_0 are to be independent.

Hence, we have

$$y_1 \not\equiv 0 \pmod{p}. \quad (10)$$

The number of solutions of the above conditions is

$$N = p^6(p-1)^2.$$

Section 10.

$$P^{p^2} = Q^p = R^p = 1, \quad R^{-1}PR = PQ, \quad PQ = QP, \quad RQ = QR,$$

The transformation formulæ for this group are:

$$P^x R^z = R^z P^x Q^{xz}, \quad (1)$$

$$R^z P^x = P^x Q^{-xz} R^z, \quad (2)$$

$$P^x Q^y R^z = R^z P^x Q^{y+xz}, \quad (3)$$

$$[P^x Q^y R^z]^k = R^{kz} P^{kx} Q^{ky + \frac{k(k+1)}{2}xz}, \quad (4)$$

$$P_0^{p^2} = 1, \quad \therefore x \not\equiv 0 \pmod{p}, \quad (5)$$

$$Q_0^p = 1, \quad x_1 \equiv 0 \pmod{p}, \quad (6)$$

$$R_0^p = 1, \quad x_2 \equiv 0 \pmod{p}. \quad (7)$$

Let $x_1 = x'p$ and $x_2 = x''p$,

$$Q_0^{-1}P_0Q_0 = P_0, \quad \therefore z_1 \equiv 0 \pmod{p}, \quad (8)$$

$$R_0^{-1}P_0R_0 = P_0Q_0, \quad \therefore \begin{cases} y_1 \equiv xz_2 \pmod{p}, \\ x'p \equiv 0 \pmod{p^2}. \end{cases} \quad (9)$$

$$(10)$$

Since $z_1 \equiv 0 \pmod{p}$ and $x_1 = 0$, we must have

$$y_1 \not\equiv 0 \pmod{p}, \quad (11)$$

and hence

$$z_2 \not\equiv 0 \pmod{p}. \quad (12)$$

Let $P_0^k Q_0^k R_0^k = 1$. The transformation formulæ applied to this give a set of impossible congruences. The above generators then are independent and whether p is odd or even

$$N = p^5(p-1)^2.$$

Sections 11, 12, 13, $p > 3$.

$$P^{p^2} = 1, \quad Q^p = 1, \quad R^p = 1, \quad Q^{-1}PQ = P^{1+p}, \quad RPQ = PR, \quad R^{-1}QR = P^{rp}Q.$$

The transformation formulæ are:

$$\left. \begin{aligned} Q^y R^z &= R^z Q^y P^{ryzp} \\ R^z Q^y &= P^{-ryzp} Q^y R^z \end{aligned} \right\} \quad (1)$$

$$\left. \begin{aligned} P^x Q^y &= Q^y P^{x(1+p)^y} \\ Q^y P^x &= P^{x(1+p)^{-y}} Q^y \end{aligned} \right\} \quad (2)$$

$$\left. \begin{aligned} P^x R^z &= R^z P^{x - \frac{zx(x-1)}{2} p + \frac{z(z-1)}{2} r x p} Q^{xz} \\ R^z P^x &= P^{x + \frac{zx(x-1)}{2} p + \frac{z(z+1)}{2} r x p} Q^{-xz} R^z \end{aligned} \right\} \quad (3)$$

$$R^z P^x Q^y = P^{x + \frac{zx(x-1)}{2} p + \frac{z(z+1)}{2} r x p - r y z p} Q^{y - xz} R^z \quad (4)$$

$$[P^x Q^y R^z]^k = P^{kx - \frac{k(k-1)}{2} x y p + \frac{k(k-1)(k-2)}{12} x^2 z p + \frac{k(k-1)}{2} \cdot \frac{zx(x-1)}{2} p + \frac{r x p}{2} \left[\frac{k(k-1)(2k-1)}{12} z^2 + \frac{k(k-1)}{2} z \right]} Q^{ky - \frac{k(k-1)}{2} xz} R^{kz}. \quad (5)$$

The above formulæ hold for groups 11, 12 and 13, according as r is a non-residue (mod p) unity or zero.

(1) r is a non-residue (mod p). P_0, Q_0 and R_0 being the new generators:

$$P_0^{p^2} = 1, \therefore x \not\equiv 0 \pmod{p}, \quad (1)$$

$$Q_0^p = 1, \therefore x_1 \equiv 0 \pmod{p}, \quad (2)$$

$$R_0^p = 1, \therefore x_2 \equiv 0 \pmod{p}. \quad (3)$$

Let $x_1 = x' p$ and $x_2 = x'' p$.

$$R_0^{-1} P_0 R_0 = P_0 Q_0, \therefore y_1 \equiv x z_2 \pmod{p}. \quad (4)$$

$$x y_2 - r z y_2 - z_2 \frac{x(x-1)}{2} + \frac{z_2(z_2-1)}{2} r x + z_2 r y \equiv x' - r z y_1 \pmod{p}. \quad (5)$$

$$Q_0^{-1} P_0 Q_0 = P_0^{1+p}, \therefore \begin{cases} z_1 \equiv 0 \pmod{p}, \\ x \equiv x y_1 - r z y_1 \pmod{p}, \end{cases} \quad (6)$$

$$R_0^{-1} Q_0 R_0 = P_0^{rp} Q_0, \therefore x \equiv y_1 z_2 \pmod{p}. \quad (8)$$

The above conditions are sufficient to insure that the new generators be independent. For a consideration of $P_0^h Q_0^k R_0^m = 1$, leads to a set of congruences inconsistent with the above. The above congruences yield $2p^4(p-1)$ sets of values. Hence,

$$N = 2p^4(p-1).$$

(2) $r=1$. Set $r=1$, in the above congruences, and again,

$$N = 2p^4(p-1).$$

(3) $r=0$. Set $r=0$, in the above congruences, and

$$N = 2p^5.$$

Sections 11, 12, 13, $p=3$.

$$P^{p^2} = 1, Q^p = 1, R^p = P^{pa}, Q^{-1} P Q = P^{1+p}, R^{-1} P R = P Q^\beta, R^{-1} Q R = Q.$$

The transformation formulæ for these groups are:

$$\left. \begin{aligned} P^x Q^y &= Q^y P^{x(1+p)^y} \\ Q^y P^x &= P^{x(1+p)^{-y}} Q^y \end{aligned} \right\} \quad (1)$$

$$\left. \begin{aligned} P^x R^z &= R^z P^{x - z\beta p \frac{x(x-1)}{2}} Q^{z\beta x} \\ R^z P^x &= P^{x + z\beta p \frac{x(x-1)}{2}} Q^{y - z\beta x} R^z \end{aligned} \right\} \quad (2)$$

$$P^x Q^y R^z = R^z P^{x-z\beta p \frac{x(x-1)}{2}} Q^{y+\beta z x}, \quad (3)$$

$$[P^x Q^y R^z]^k = P^{kx - \frac{k(k-1)}{2}xy p + \frac{k(k-1)(k-2)}{6}x^2 z \beta p + \frac{k(k-1)}{2}z\beta p \frac{x(x-1)}{2}} Q^{ky - \frac{k(k-1)}{2}\beta z x} R^{kz}. \quad (4)$$

The above formulæ hold for groups 11, 12 and 13, when $p=3$.

(1) $p=3$, $\alpha=0$, $\beta=1$. P_0, Q_0 and R_0 being the new generators.

$$P_0^9=1, \therefore x+x^2 z \not\equiv 0 \pmod{3}, \quad (1)$$

$$Q_0^3=1, \therefore x_1+x_1^2 z_1 \equiv 0 \pmod{3}, \quad (2)$$

$$R_0^3=1, \therefore x_2+x_2^2 z_2 \equiv 0 \pmod{3}. \quad (3)$$

$$Q_0^{-1} P_0 Q_0 = P_0^{1+3}, \therefore x z_1 - x_1 z \equiv 0 \pmod{3}, \quad (4)$$

$$x+x^2 z \equiv x y_1 - x_1 y + z \frac{x_1(x_1-1)}{2} - z_1 \frac{x(x-1)}{2} \pmod{3}, \quad (5)$$

$$R_0^{-1} P_0 R_0 = P_0 Q_0, \therefore z_1 \equiv 0 \pmod{3}, \quad (6)$$

$$y_1 - x_1 z \equiv z_2 x - x_2 z \pmod{3}, \quad (7)$$

$$x_1 - 3x_1 y + 3z \frac{x_1(x_1-1)}{2} \equiv 3x y_2 - 3x_2 y + 3z \frac{x_2(x_2-1)}{2} - 3z_2 \frac{x(x-1)}{2} \pmod{9}, \quad (8)$$

$$R_0^{-1} Q_0 R_0 = Q_0, \therefore x_1 z_2 \equiv 0 \pmod{3}, \quad (9)$$

$$x_1 y_2 - x_2 y_1 - z_2 x_1 \frac{(x_1-1)}{2} \equiv 0 \pmod{3}. \quad (10)$$

Before solving the above congruences can be reduced to the equivalent

$x \not\equiv 0$, $z_1 \equiv 0$, $x_1 \equiv 0$, $x_2 \equiv 0$, $z_2 \not\equiv 0$, $x+x^2 z \equiv x y_1$, $y_1 \equiv x z_2$, $y_1 \not\equiv 0$,

$$x' \equiv x y_2 + z_2 x \frac{(x-1)}{2}, \text{ all taken } \pmod{3}.$$

The congruences obtained from $P_0^h Q_0^k R_0^l = 1$ are not consistent with those obtained from the defining relations. Hence, P_0, Q_0 and R_0 are independent, without further condition

$$N = 2^2 3^4.$$

(2) $p=3$, $\alpha=1$, $\beta=-1$.

$$P^9=Q^3=1, R^3=P^3, Q^{-1}PQ=P^{1+3}, R^{-1}PR=PQ^{-1}, QR=RQ.$$

$$P_0^9=1, \therefore x-x^2 z + z \not\equiv 0 \pmod{3}, \quad (1)$$

$$Q_0^3=1, \therefore x_1-x_1^2 z + z_1 \equiv 0 \pmod{3}, \quad (2)$$

$$R_0^3=P_0^3, \therefore x_2-x_2^2 z_2 + z_2 \equiv x-x^2 z + z \pmod{3}, \quad (3)$$

$$Q_0^{-1} P_0 Q_0 = P_0^{1+3}, \therefore z_1 x - x_1 z \equiv 0 \pmod{3}, \quad (4)$$

$$x-x^2 z + z \equiv x y_1 - x_1 y + z \frac{x_1(x_1-1)}{2} - z_1 x \frac{(x-1)}{2} \pmod{3}, \quad (5)$$

$$R_0^{-1} P_0 R_0 = P_0 Q_0^{-1}, \therefore z_1 \equiv 0 \pmod{3}, \quad (6)$$

$$y_1 \equiv z_2 x - x_2 z \pmod{3}, \quad (7)$$

$$-(x_1+z_1) \equiv 3x y_2 - 3x_2 y + 3z_2 x \frac{(x-1)}{2} - 3z x_2 \frac{(x_2-1)}{2} \pmod{9}, \quad (8)$$

$$R_0^{-1} Q_0 R_0 = Q_0, \therefore x_2 y_1 \equiv 0 \pmod{3}, \quad (9)$$

$$\therefore x_2 \equiv 0 \text{ and } y_1 \not\equiv 0 \pmod{3}. \quad (10)$$

Let $z_1 = 3z'$, $x_1 = 3x'$, $x_2 = 3x''$.

A consideration of $P_0^k Q_0^h R_0^m = 1$ gives no further conditions to be imposed on the exponents to insure the independence of P_0, Q_0, R_0 .

The above congruences can be reduced to the equivalent set $y_1 \not\equiv 0$, $x_2 \equiv 0$, $x_1 \equiv 0$, $z_1 \equiv 0$, $z_2 \not\equiv 0$, $x \not\equiv 0$, $x - x^2 z + z \equiv z_2$, $x y_1 \equiv x - x^2 z + z \equiv z_2$, $y_1 \equiv z_2 x$, $x' + z' \equiv -x y_2 - z_2 x \frac{(x-1)}{2}$, all (mod 3),

$$\therefore N = 2 \cdot 3^8.$$

$$(3) \quad p=3, \alpha=-1, \beta=-1.$$

$$P^9=1, Q^3=1, R^3=P^{-3}, Q^{-1}PQ=P^{1+3}, R^{-1}PR=PQ^{-1}, RQ=QR.$$

$$P_0^9=1, \quad x-x^2z-z \not\equiv 0 \pmod{3}, \quad (1)$$

$$Q_0^3=1, \quad x_1-x_1^2-z \equiv 0 \pmod{3}, \quad (2)$$

$$R_0^3=P_0^3, \quad x_2-x_2^2-z_2 \equiv -x+x^2z+z \pmod{3}, \quad (3)$$

$$Q_0^{-1}P_0Q=P_0^{1+3}, \quad x y_1 \equiv x-x^2z-z \pmod{3}, \quad (4)$$

$$R_0^{-1}P_0R_0=P_0Q_0^{-1}, \quad \therefore z_1 \equiv 0 \pmod{3}, \quad (5)$$

$$y_1 \equiv z_2 x - x_2 z \pmod{3}, \quad (6)$$

$$z' - x' \equiv x y_2 - x_2 y + z_2 x \frac{(x-1)}{2} - z x_2 \frac{(x_2-1)}{2} \pmod{3}, \quad (7)$$

$$R_0^{-1}Q_0R_0=Q_0, \quad \therefore x_2 y_1 \equiv 0 \pmod{3}. \quad (8)$$

Now, $y_1 \not\equiv 0 \pmod{3}$, else P_0 and Q_0 are permutable operations,

$$\therefore x_2 \equiv 0, z_2 \not\equiv 0.$$

The relation $P_0^h Q_0^k R_0^l = 1$ gives no further conditions. Hence, the above relations are sufficient for the independence of P_0, Q_0, R_0 . The above congruences reduce to the simpler set $x_1 \equiv 0$, $z_1 \equiv 0$, $x_2 \equiv 0$, $z_2 \not\equiv 0$, $y_1 \not\equiv 0$, $x \not\equiv 0$, $y_1 \equiv z_2 x$, $z_2 \equiv x - x^2 z - z$, $x y_1 \equiv z_2 \equiv x - x^2 z - z$, $z' - x' \equiv x y_2 + z_2 x \frac{(x-1)}{2}$, all (mod 3), and where $x_1 = 3x'$, $x_2 = 3x''$, $z_1 = 3z'$. We easily deduce from the above $x^2 \equiv 1$, $z_2 \equiv x + z$, $y_1 \equiv 1 + xz$, and find the number of solutions to be

$$N = 2^2 \cdot 3^7.$$

Section 14.

$$P^p=1, Q^p=1, R^p=1, S^p=1, R^{-1}PR=P, R^{-1}QR=Q, Q^{-1}PQ=P, S^{-1}PS=P, S^{-1}QS=Q, S^{-1}RS=RP.$$

The transformation formulæ are:

$$R^z S^w = S^w R^z P^{wz}, \quad (1)$$

$$S^w R^z = P^{-wz} R^z S^w, \quad (2)$$

$$P^x Q^y R^z S^w = P^{x+wz} Q^y S^w R^z, \quad (3)$$

$$[P^x Q^y R^z S^w]^k = P^{kx - k \frac{(k-1)}{2} wz} Q^{ky} R^{kz} S^{kw}. \quad (4)$$

Every operation of the group is of order p , p being an odd prime.

$P_0^p = Q_0^p = R_0^p = S_0^p = 1$ without restriction on the exponents.

$$S_0^{-1} R_0 S_0 = R_0 P_0 \quad \therefore \begin{cases} w \equiv z \equiv y \equiv 0, \\ x \equiv w_3 z_2 - z_3 w_2 \not\equiv 0, \end{cases} \quad (5)$$

$$S_0^{-1} Q_0 S_0 = Q_0, \quad \therefore w_3 z_1 - z_3 w_1 \equiv 0, \quad (6)$$

$$S_0^{-1} P_0 S_0 = P_0, \quad \therefore w_3 z - z_3 w \equiv 0, \quad (7)$$

$$R_0^{-1} Q_0 R_0 = Q_0, \quad \therefore w_2 z_1 - z_2 w_1 \equiv 0, \quad (8)$$

$$R_0^{-1} P_0 R_0 = P_0, \quad \therefore w_2 z - z_2 w \equiv 0, \quad (9)$$

$$Q_0^{-1} P_0 Q_0 = P_0, \quad \therefore w_1 z - z_1 w \equiv 0. \quad (10)$$

The relation $P_0^h Q_0^k R_0^l S_0^m = 1$ gives a set of congruences which cannot be satisfied if we impose the further condition

$$y_1 \not\equiv 0, \quad (11)$$

This last condition, $y_1 \not\equiv 0$, together with those obtained from the defining relations, insures P_0, Q_0, R_0, S_0 independent. The number of their solutions is

$$N = p^6 (p-1)^3 (p+1).$$

Section 15, $p > 3$.

$$P^p = Q^p = R^p = S^p = 1, \quad S^{-1} R S = R Q, \quad S^{-1} Q S = Q P, \quad S^{-1} P S = P, \quad R^{-1} Q R = Q, \\ R^{-1} P R = P, \quad Q^{-1} P Q = P.$$

The transformation formulæ are:

$$Q^y S^w = S^w Q^y P^{wy}, \quad (1)$$

$$R^z S^w = S^w R^z Q^{wz} P^{w \frac{(w-1)z}{2}}, \quad (2)$$

$$[P^x Q^y R^z S^w]^k = P^{kx - k \frac{(k-1)}{2} wy + \frac{z}{2} [k \frac{(k-1)}{6} (2k-1) w^2 + k \frac{(k-1)}{2} w]} Q^{ky - k \frac{(k-1)}{2} wz} R^{kz} S^{kw}, \quad (3)$$

$$P_0^p = Q_0^p = R_0^p = S_0^p = 1, \text{ without restrictions.}$$

$$S_0^{-1} P_0 S_0 = P_0, \quad \therefore w_1 \equiv z_1 \equiv y_1 \equiv w_4 z_4 \equiv 0, \quad x \not\equiv 0, \quad (4)$$

$$R_0^{-1} Q_0 R_0 = Q_0, \quad \therefore w_2 \equiv z_2 \equiv y_2 w_3 \equiv 0, \quad (5)$$

$$S_0^{-1} Q_0 S_0 = Q_0 P_0, \quad \therefore x_1 \equiv y_2 w_4, \quad (6)$$

$$S_0^{-1} R_0 S_0 = R_0 Q_0, \quad \therefore \begin{cases} y_2 \equiv w_4 z_3, \\ x_2 \equiv y_3 w_4 + w_4 \frac{(w_4+1)}{2} z_3. \end{cases} \quad (7)$$

$$Q_0^{-1} P_0 Q_0 = P_0. \quad \text{This is satisfied without restriction.} \quad (8)$$

The relation $P_0^h Q_0^k R_0^l S_0^m = 1$ is impossible from the above conditions.

The generators P_0, Q_0, R_0, S_0 are independent, and the number of solutions of the above conditions is

$$N = p^4 (p-1)^2.$$

Section 15, $p = 3$.

$$P^p = Q^p = R^p = 1, \quad Q^{-1}PQ = P, \quad R^{-1}PR = PQ, \quad R^{-1}QR = P^{p(p-1)}Q.$$

The transformation formulæ are:

$$Q^y R^z = R^z P^{zy^{p(p-1)}} Q^y, \quad (1)$$

$$P^x R^z = R^z P^{x+xz\frac{(z-1)}{2}p(p-1)} Q^{xz}, \quad (2)$$

$$P^x Q^y R^z = R^z P^{x+xz\frac{(z-1)}{2}p(p-1)+zy^{p(p-1)}} Q^{y+xz}, \quad (3)$$

$$[P^x Q^y R^z]^k = P^{kx+p\frac{(p-1)}{2}xz^2k\frac{(k-1)(2k-1)}{6}+p\frac{(p-1)}{2}xz k\frac{(k-1)}{2}-p(p-1)yzk\frac{(k-1)}{2}} Q^{ky-xzk\frac{(k-1)}{2}} R^{kz}. \quad (4)$$

$$P_0^3 = 1, \quad \therefore x \not\equiv 0, \quad (5)$$

$$Q_0^3 = 1, \quad \therefore x_1 \equiv 0, \quad x_1 = 3x', \quad (6)$$

$$R_0^3 = 1, \quad \therefore x_2 \equiv 0, \quad x_2 = 3x'', \quad (7)$$

$$R_0^{-1}Q_0R_0 = P_0^{-3}, \quad \therefore 2(y_1z_2 - y_2z_1) \equiv x(2+z^2), \quad (8)$$

$$R_0^{-1}P_0R_0 = P_0Q_0, \quad \therefore \begin{cases} z_1 \equiv 0, \\ y_1 \equiv xz_2, \end{cases} \quad (9)$$

$$xz_2(z_2-1) + 2[yz_2 - zy_2 + y_1z] \equiv x', \quad (10)$$

$$Q_0^{-1}P_0Q_0 = P_0, \quad \therefore y_1z \equiv 0. \quad (11)$$

$$Q_0^{-1}P_0Q_0 = P_0, \quad \therefore y_1z \equiv 0. \quad (12)$$

The relation $P_0^h Q_0^k R_0^l = 1$ leads to a set of congruences inconsistent with those obtained from the defining relations of the group.

The above congruences are all (mod 3). The number of solutions is

$$N = 540.$$

Section 16.

The order of the groups of isomorphisms of the abelian groups is the same whether p is an odd or even prime, and so requires no further investigation. The order of the groups of isomorphisms of the non-abelian groups in Sections 6, 8, 9, 10 holds when p is odd or even. The group Section 7 required independent investigation when p is even. The following sections are given to the investigation of groups which exist only when $p=2$.

Section 17.

$$P^4 = 1, \quad Q^4 = 1, \quad R^2 = 1, \quad Q^{-1}PQ = P^{-1}, \quad Q^2 = P^2, \quad QR = RQ, \quad PR = RP.$$

The following transformation formulæ hold:

$$P^x Q^y = Q^y P^{x(1+2y)}, \quad (1)$$

$$[P^x Q^y]^k = P^{kx-2xyk\frac{(k-1)}{2}} Q^{ky}, \quad (2)$$

$$[P^x Q^y R^z]^k = P^{kx-2xyk\frac{(k-1)}{2}} Q^{ky} R^{kz}. \quad (3)$$

$$P_0^4 = Q_0^4 = 1, \quad \text{without condition.}$$

$$P_0^2 = Q_0^2, \quad \therefore x - xy + y \equiv x_1 - x_1y_1 + y_1 \not\equiv 0 \pmod{2}, \quad (4)$$

$$R_0^2=1, \quad \therefore x_2-x_2y_2+y_2 \equiv 0 \pmod{2}, \quad (5)$$

$$Q_0^{-1}P_0Q_0=P_0^{-1}, \quad \therefore xy_1-x_1y \equiv x-xy+y \pmod{2}, \quad (6)$$

$$R_0^{-1}Q_0R_0=Q_0, \quad \therefore x_1y_2-x_2y_1 \equiv 0 \pmod{2}, \quad (7)$$

$$R_0^{-1}P_0Q_0=P_0, \quad \therefore xy_2-x_2y \equiv 0 \pmod{2}. \quad (8)$$

Now, (6) is the condition that (7) and (8) have only zero solutions for x_2 and y_2 ,

$$\therefore x_2 \equiv 0, \quad y_2 \equiv 0 \pmod{2}. \quad (9)$$

Suppose the relation to exist

$$P_0^h Q_0^k R_0^l = 1.$$

This requires $z_2 \equiv 0 \pmod{2}$. Hence, if $z_2 \not\equiv 0$, the above generators are independent,

$$\therefore z_2 \not\equiv 0 \pmod{2}. \quad (10)$$

The number of solutions of these congruences is:

$$N = 3 \cdot 2^7.$$

Section 18.

$$P^8=1, \quad Q^2=1, \quad Q^{-1}PQ=P^{-1}=P^7. \\ P^x Q^y = Q^y P^{x(1+4y+2y^2)}, \quad (1)$$

$$Q^y P^x = P^{x(1-4y+2y^2)} Q^y, \quad (2)$$

$$[P^x Q^y]^k = P^{kx+2xy} \left[\frac{k(k-1)(2k-1)}{6} y - k(k-1) \right] Q^{ky}. \quad (3)$$

There are four operations of order 8, and they are the odd powers of P
Let

$$P_0 = P^x,$$

$$Q_0 = P^{x_1} Q,$$

and it is easy to see that

$$N = 2^5.$$

Section 19.

$$P^8=1, \quad Q^2=1, \quad Q^{-1}PQ=P^3. \\ P^x Q^y = Q^y P^{x(1+2y^2)}, \quad (1)$$

$$Q^y P^x = P^{x(1+2y^2)} Q^y, \quad (2)$$

$$[P^x Q^y]^k = P^{kx+2k \frac{(k-1)(2k-1)}{6} xy^2} Q^{ky}. \quad (3)$$

There are only four operations of order 8, and they are the powers of P , not congruent to zero. Let

$$P_0 = P^x,$$

$$Q_0 = P^{x_1} Q^{y_1}.$$

$$P_0^8 = [P^x]^8 = P^{8x} = 1, \quad \therefore x \not\equiv 0 \pmod{2}. \quad (4)$$

$$Q_0^2 = 1, \quad \therefore x_1(1+y_1^2) \equiv 0 \pmod{4}.$$

Since $y_1 \not\equiv 0$, for if it were P_0 and Q_0 would be dependent, we must have $x_1 \equiv 0 \pmod{2}$ and $y_1 \equiv 1 \pmod{2}$. Hence,

$$N = 2^4.$$

Section 20.

$$P^8=1, Q^4=1, Q^{-1}PQ=P^{-1}=P^7, Q^2=P^4. \\ P^x Q^y = Q^y P^{x(1+4y+2y^2)}, \quad (1)$$

$$Q^y P^x = P^{x(1-4y+2y^2)} Q^y, \quad (2)$$

$$[P^x Q^y]^k = P^{kx+2xy} \left[\frac{k(k-1)(2k-1)}{6} y - k(k-1) \right] Q^{ky}. \quad (3)$$

There are four operations of order 8, and they are the odd powers of P .

Let

$$P_0 = P^x,$$

$$Q_0 = P^{x_1} Q,$$

$$P_0^8=1, \therefore x \not\equiv 0 \pmod{2}, \quad (4)$$

$$Q_0^4=1. \quad \text{This is satisfied without condition.}$$

$$Q_0^2=P_0^4, \therefore x \equiv 1 \pmod{2}. \quad (5)$$

$$N = 2^5.$$